UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/791,160 | 03/01/2004 | Mitchell B. Oliver | 020294 | 3432 |

23696 7590 07/09/2010

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

| EXAMINER | |
|---|---|
| PATEL, DHAIRYA A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2451 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 07/09/2010 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/791,160 | OLIVER ET AL. | |
| | Examiner | Art Unit | |
| | Dhairya A. Patel | 2451 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *12 April 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

**DETAILED ACTION**

1. This action is responsive to appeal brief filed on 4/12/2010. Claims 1-24 are subject to examination. The after-final amendment filed on 12/4/2009 has been entered.

2.

In view of the Appeal Brief filed on 4/12/2010, PROSECUTION IS HEREBY REOPENED. A non-final Office Action is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 19-21 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As per claim 19, it states "In computer readable storage medium, a program when executed by a wireless computer device…downloading through a wireless connection…executing the application...with the download manager..". The claim is drawn to "computer readable storage medium". The specification of the current application in paragraph 34 states that "computer readable medium such a memory of the computer platform. The instructions can reside in various types of signal-bearing or data storage primary media". Furthermore it defines media as "digital and analog transmission media". Therefore, the claim as whole covers both transitory and non-transitory media. A transitory medium does not fall into any of the 4 categories of invention (process, machine, manufacture or composition of matter).

As per claim 20-21 depend on rejected claim 19, therefore rejected under same basis.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

***Claims 1-7,9-14,16-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koskimies et al. U.S. Patent Publication # 2004/0081110 (hereinafter Koskimies) in view of Brody et al. U.S. Patent Publication # 2001/0051928 (hereinafter Brody)***

As per claim 1, Koskimies teaches a computer device (having wireless communication capability, comprising:

-a wireless communication portal for selectively sending and receiving data across a wireless network (Paragraph 50, 52, 66); **NOTE:** The reference teaches having a WAP page of the sound download service at the content server which has midlets (i.e. sending/receiving data) and downloading a midlet across the network through infrared or Bluetooth functionality.

-a computer platform (Fig. 1 element 110) including a resident application environment and selectively download applications to the platform through the portal (Paragraph 50, 56, 59) the resident application environment configured to selectively download application (Paragraph 50,56) that comply with a predefined security protocol (Paragraph 78,79,80 ); **NOTE:** The reference teaches having mobile device (computer platform) which includes java "mobile information device applets (midlets)" which are downloaded through a WAP page of the sound download service (i.e. portal page). In Paragraph 59, it states selecting one or multiple midlets by the user to download at the mobile device (selectively download applications). In Paragraph 78, 79, 80, it teaches that downloading can be done by encrypting before downloading and decrypting by a particular target (i.e. comply with a predefined security protocol). According the specification of the current invention, it states applications are midlets or applets. Therefore, Koskimies teaches midlets/applets.

-a data store (i.e. content server or storage on the mobile device) in communication with the computer platform and selectively sending data to and

receiving data from the computer platform (Paragraph 50, 53); **NOTE:** The reference teaches midlet will retrieve a list of available content items from the content server (i.e. data store) which is in communication with the mobile device. After selecting a content item (i.e. sound clip), the midlet can effect charging such as by sending an SMS and can then download the content and immediately forward it to the limited device (selectively sending data to and receiving data from the computer platform).

- a download manager resident on the computer platform that at least selectively downloads applications through the portal that do not comply with the predefined security protocol (Paragraph 78, 83) **NOTE:** The reference states downloading content to a device unauthorized by the content creator, and downloading unauthorized content (i.e. unauthorized by the device maker) to the device i.e. downloading application that does not comply with the security protocol

Koskimies states a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol but Brody particularly points out a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol (Paragraph 22). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Brody's teaching gin Koskimies's teaching to come up with downloading application which does not comply with security protocol. The motivation for doing so would be sometimes downloading

application which does not comply with security protocol are safe, therefore there is no harm to the user's computer in downloading them.

As per claim 2, Koskimies and Brody teaches the device of claim 1, but Koskimies further teaches wherein the download manager (i.e. sound download service on the WAP page) exists within resident application environment and uses an existing application download interface (Paragraph 50, 66).

As per claim 3, Koskimies and Brody teaches the device of claim 1, but Koskimies further teaches wherein the downloaded application is immediately executed (Paragraph 50, 59).

As per claim 4, Koskimies and Brody teaches the device of claim 1, but Koskimies further teaches wherein a downloaded application that does not comply with the predefined security protocol is stored (Paragraph 78, 83), and but Koskimies fails to teach the stored application is executed through the download manager. Brody teaches the stored application is executed through the download manager (Paragraph 22). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Brody's teaching in Koskimies's teaching to come up with executing the application through download manager. The motivation for doing so would to test/verify the application by executing whether it is safe or malicious.

As per claim 5, Koskimies and Brody teaches the device of claim 1, but Brody further teaches wherein the download manager further manages executing the downloaded application that does not comply with the predefined security protocol (Paragraph 22).

As per claim 6, Koskimies and Brody teaches the device of claim 4, but Koskimies also teaches wherein the download manager further manages storage of the downloaded application that does not comply with the predefined security protocol in the data store (Paragraph 83)

As per claim 7, Koskimies and Brody teaches the device of claim 1, but Koskimies further teaches wherein the predefined security protocol is verifying the origination of the application (Paragraph 50, 56, 78, 79).

As per claim 9, Koskimies and Brody teaches the device of claim 5, but Koskimies further teaches wherein the download manager executes the downloaded application that does not comply with the predefined security protocol outside of the resident application environment (Paragraph 78, 83).

As per claim 10, Koskimies teaches a computer device having wireless communication capability, comprising: a wireless communication means for selectively sending and receiving data across a wireless network (Paragraph 50, 52, 66); **NOTE:** The reference teaches having a WAP page of the sound download service at the content server which has midlets (i.e. sending/receiving data) and downloading a midlet across the network through infrared or Bluetooth functionality.

a computer means selectively downloading applications through the wireless communication means, the computer means configured to selectively download application (Paragraph 50,56) that comply with a predefined security protocol (Paragraph 78,79,80); **NOTE:** The reference teaches having mobile device (computer platform) which includes java "mobile information device

applets (midlets)" which are downloaded through a WAP page of the sound download service (i.e. portal page). In Paragraph 78, 79, 80, it teaches that downloading can be done by encrypting before downloading and decrypting by a particular target (i.e. comply with a predefined security protocol). According the specification of the current invention, it states applications are midlets or applets. Therefore, Koskimies teaches midlets/applets.

-a means for selectively downloading application through the wireless communications means that do no comply with the predefined security protocol (Paragraph 50, 78, 83) **NOTE:** The reference states downloading content to a device unauthorized by the content creator, and downloading unauthorized content (i.e. unauthorized by the device maker) to the device i.e. downloading application that does not comply with the security protocol. The downloading is done on the phone using infrared or Bluetooth communication (i.e. wireless communication)

Koskimies states selectively downloading application through the wireless communications means that do no comply with the predefined security protocol but Brody particularly points out selectively downloading application through the wireless communications means that do no comply with the predefined security protocol (Paragraph 22). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Brody's teaching gin Koskimies's teaching to come up with downloading application which does not comply with security protocol. The motivation for doing so would be sometimes downloading application which does not comply with security

protocol are safe, therefore there is no harm to the user's computer in downloading them

As per claim 11, Koskimies teaches a method of selectively downloading through a wireless connection to a computer device an application that does not comply with a predefined security protocol for use at that computer device (Paragraph 78, 83), comprising the steps of: downloading from a wireless network to a computer platform of the computer device an application that does not comply with a predefined security protocol for use at that computer device (Paragraph 50, 78, 83) **NOTE:** The reference states downloading content to a device unauthorized by the content creator, and downloading unauthorized content (i.e. unauthorized by the device maker) to the device i.e. downloading application that does not comply with the security protocol. The downloading is done on the phone using infrared or Bluetooth communication (i.e. wireless communication)

-the computer platform including a resident application environment for downloading and executing applications utilizing a predefined security protocol for at least downloading an application (Paragraph 50, 53, 59), the downloading of the non-complying application occurring through the use of a download manager resident on the computer platform; (Paragraph 78, 83); **NOTE:** The reference teaches having mobile device (computer platform) which includes java "mobile information device applets (midlets)" which are downloaded through a WAP page of the sound download service (i.e. portal page). In Paragraph 59, it states selecting one or multiple midlets by the user to download at the mobile

device (selectively download applications). In Paragraph 78, 79, 80, it teaches that downloading can be done by encrypting before downloading and decrypting by a particular target (i.e. comply with a predefined security protocol). According the specification of the current invention, it states applications are midlets or applets. Therefore, Koskimies teaches midlets/applets.

-executing the application at the computer device with the download manager (i.e. sound download service on the WAP page) (paragraph 50, 59, 66). **NOTE:** The reference teaches executing the midlet after it is downloaded at the mobile device after user selecting the particular midlet/program to be downloaded (Paragraph 59).

Although Koskimies teaches an application that does not comply with a predefined security protocol (Paragraph 78, 83), Brody explicitly points out that downloading from a wireless network to a computer platform of the computer device an application that does not comply with a predefined security protocol for use at that computer device (Paragraph 22) and the downloading of the non-complying application occurring through the use of a download manager resident on the computer platform (Paragraph 22). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Brody's teaching gin Koskimies's teaching to come up with downloading application which does not comply with security protocol. The motivation for doing so would be sometimes downloading application which does not comply with security protocol are safe, therefore there is no harm to the user's computer in downloading them

As per claim 12, Koskimies and Brody teaches the method of claim 11, but Koskimies further teaches wherein the download manager (i.e. sound download service on the WAP page) exists within resident application environment and the step of downloading uses an existing application download interface (Paragraph 50, 66).

As per claim 13, Koskimies and Brody teaches the method of claim 11, but Koskimies further teaches further comprising the steps of: storing, with the download manager the downloaded application that does not comply with the predefined security protocol (Paragraph 83). Koskimies does not teach executing the stored application through the download manager. Brody teaches the stored application is executed through the download manager (Paragraph 22). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Brody's teaching in Koskimies's teaching to come up with executing the application through download manager. The motivation for doing so would to test/verify the application by executing whether it is safe or malicious.

As per claim 14, Koskimies and Brody teaches the method of claim 11, but Koskimies further teaches further comprising the step of verifying the nature of the downloaded application as the predefined security protocol (Paragraph 50, 56, 78, 79).

As per claim 16, Koskimies and Brody teaches the method of claim 11, but Koskimies further teaches wherein the step of executing the downloaded

application with the download manager occurs outside of the resident application environment (Paragraph 50, 59).

As per claim 17, Koskimies and Brody teaches the method of claim 11, but Brody further teaches further comprising the step of downloading the download manager to the computer platform of the computer device after a request to download an application that does not comply with a predefined security protocol has been made (Paragraph 78, 83), and prior to the step of downloading the requested application (Paragraph 83).

As per claim 18, Koskimies teaches a method of selectively downloading through a wireless connection to a computer device an application that does not comply with a predefined security protocol for use at that computer device, comprising the steps of: a step for downloading through the wireless communication to a computer platform of the computer device an application that does not comply with a predefined security protocol for use within a resident application environment at that computer device (Paragraph 50, 78, 83) **NOTE:** The reference states downloading content to a device unauthorized by the content creator, and downloading unauthorized content (i.e. unauthorized by the device maker) to the device i.e. downloading application that does not comply with the security protocol. The downloading is done on the phone using infrared or Bluetooth communication (i.e. wireless communication)

-a step for executing the downloaded application at the computer device outside of the resident application environment (Paragraph 78, 83).

Although Koskimies teaches downloading through the wireless communication to a computer platform of the computer device an application that does not comply with a predefined security protocol for use within a resident application environment at that computer device but Brody further teaches downloading through the wireless communication to a computer platform of the computer device an application that does not comply with a predefined security protocol for use within a resident application environment at that computer device (Paragraph 22). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Brody's teaching gin Koskimies's teaching to come up with downloading application which does not comply with security protocol. The motivation for doing so would be sometimes downloading application which does not comply with security protocol are safe, therefore there is no harm to the user's computer in downloading them.

As per claim 19, it teaches same limitation as claim 11, therefore rejected under same basis.

As per claim 20, Koskimies and Brody teaches the program of claim 19, but Koskimies further teaches wherein the download manager (i.e. sound download service on the WAP page) is resident on the computer platform (Paragraph 50)

As per claim 21, Koskimies teaches the program of claim 19, wherein the download manager is loaded to the computer platform after a request to download of an application that does not comply with a predefined security protocol (Paragraph 78, 83) and prior to download thereof (Paragraph 83)

As per claim 22, Koskimies and Brody teaches the computer device of claim 1, but Koskimies further teaches wherein the download manager exists within resident application environment and uses an existing application download interface (Paragraph 50, 56), and wherein the download manager further manages executing the downloaded application that does not comply with predefined security protocol (Paragraph 83).

As per claim 23, Koskimies and Brody teaches the computer device of claim 1, but Koskimies further teaches wherein the pre-defined security protocol includes an application validation requirement of the resident application environment (Paragraph 79-81)

As per claim 24, Koskimies and Brody teaches the computer device of claim 1, but Koskimies further teaches wherein the application being downloaded by the resident application environment in compliance with the pre-defined security protocol (Paragraph 79-81) and the application being downloaded by the download manager in non-compliance with the pre-defined security protocol are both stored in the data store (Paragraph 78, 83).

***Claims 8, 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koskimies et al. U.S. Patent Publication # 2004/0081110 (hereinafter Koskimies) in view of Brody et al. U.S. Patent Publication # 2001/0051928 (hereinafter Brody) further in view of Hericourt et al. U.S. Patent # 7,099,916 (hereinafter Hericourt)***

As per claim 8, Koskimies and Brody teaches the device of claim 1, but fails to further teach wherein the predefined security protocol is verifying the

presence of a certificate within the downloaded application. Hericourt teaches wherein the predefined security protocol is verifying the presence of a certificate within the downloaded application (column 10 lines 11-29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Hericourt's teaching in Koskimies and Brody's teaching to come up with verifying the presence of certificate within the downloaded application. The motivation for doing so would be to verify the identity of the application/file and make sure the it is virus free, thereby the certificate provides a virus-free certificate.

As per claim 15, Koskimies and Brody teaches the method of claim 14, but fails to teach wherein the step of verifying the nature of the downloaded application is verifying the presence of a certificate within the downloaded application. Hericourt teaches verifying the nature of the downloaded application is verifying the presence of a certificate within the downloaded application (column 10 lines 11-29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Hericourt's teaching in Koskimies and Brody's teaching to come up with verifying the presence of certificate within the downloaded application. The motivation for doing so would be to verify the identity of the application/file and make sure the it is virus free, thereby the certificate provides a virus-free certificate.

***Response to Arguments***

Applicant's arguments with respect to claims 1-22 have been considered but are moot in view of the new ground(s) of rejection.

In view of the Appeal Brief filed on 11/20/2006, PROSECUTION IS HEREBY

REOPENED. A non-final Office Action is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

***Conclusion***

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

   A). Kiessling et al. U.S. Patent # 6,901,251

   B). Stillerman et al. U.S. patent # 7,467,417/

4. A shortened statutory period for response to this action is set to expire **3 (three) months and 0 (zero) days** from the mail date of this letter. Failure to respond within the period for response will result in **ABANDONMENT** of the applicant (see 35 U.S.C 133, M.P.E.P 710.02, 710.02(b)).

5.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dhairya A. Patel whose telephone number is 571-272-5809. The examiner can normally be reached on Monday-Friday 8:00AM-5: 30PM, first Fridays OFF.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DAP
/John Follansbee/

Supervisory Patent Examiner, Art Unit 2451